11-01-04 09844466 B5

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/30	A2	(11) International Publication Number: WO 99/34554
		(43) International Publication Date: 8 July 1999 (08.07.99)

(21) International Application Number: PCT/IB98/01923

(22) International Filing Date: 3 December 1998 (03.12.98)

(30) Priority Data:
08/989,875 24 December 1997 (24.12.97) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Applicant *(for SE only)*: PHILIPS AB [SE/SE]; Kottbygatan 7, Kista, S-164 85 Stockholm (SE).

(72) Inventors: CUCCIA, David; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). EPSTEIN, Michael, A.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). PASIEKA, Michael, S.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: FAESSEN, Louis, M., H.; Internationaal Octrooibureau B.V., P.O. Box 220, NL-5600 AE Eindhoven (NL).

(81) Designated States: CN, JP, KR, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: ADMINISTRATION AND UTILIZATION OF SECRET FRESH RANDOM NUMBERS IN A NETWORKED ENVIRONMENT

(57) Abstract

In a public key cryptosystem employing the El-Gamal algorithm, secret fresh random numbers are generated at a server and private keys of users, as encrypted with a symmetric algorithm by using individual user identifying keys determined by hashing the users' respective passphrases or biometric information (fingerprint, voiceprint, retina scan, or face scan) are maintained in a store accessible to the server, and the fresh random numbers and encrypted private keys are transmitted to the user equipment when needed via a network which is not secure. In order to prevent an attacker from discovering the random numbers or employing formerly used random numbers in a block replay attack, an interchange in the nature of a challenge response protocol is employed which passes at least one secret fresh random number from the server to the user equipment while also authenticating the user to the server. In this interchange, a first random number to be distributed to the user for use in signing a document and a second random number which is to be used by the user in forming a signature of a hashing together of the first and second random numbers as part of the challenge response protocol, are supplied to the user equipment in encrypted form together with a freshness value, and a signature by the server of a hashing together of the first and second random numbers and the freshness value.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Administration and utilization of secret fresh random numbers in a networked environment.

This application is related in subject matter to an application by one of the inventors herein filed on December 19, 1997, entitled "Administration and Utilization of Private Keys in a Networked Environment".

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to methods and systems for administration and utilization of secret fresh random numbers in a networked environment, for example, for digital signature or encryption operations employing the El-Gamal algorithm.

2. Description of the Related Art

Random numbers which are secret and have not been previously used, termed herein "secret fresh random numbers" are utilized in a variety of cryptosystems. One such use is for performing either a digital signature or an encryption in a public key cryptosystem employing the El-Gamal algorithm. In public key cryptosystems a pair of a corresponding public key and a private key may be assigned for each user or client.

The need for secret fresh random numbers when the El-Gamal algorithm is employed for either digital signing or encrypting, is due to its two main weaknesses: 1) none of the random numbers can ever be known by an attacker; and 2) use of the same random number to sign or encrypt two different documents is prohibited. Failure in either case allows an attacker enough information to recover a private key used for a digital signature, or to recover items which have been encrypted using a public key. The recovery of a particular private key by an eavesdropper is considered a catastrophic failure of the system and the recovery of messages sent encrypted with a particular public key may be considered a catastrophic failure depending on the nature of the messages.

A digital signature employing the El-Gamal algorithm utilizes the private key of the signer, a secret fresh random number, and generally the result of applying a secure hash function (such as SHA-1 or RIPEMD) to one or more data items, such as documents, files, programs, or keys (which for simplicity are referred to hereinafter as "documents") to manifest the signer's origination, approval, or certification thereof. The documents to which the

signature applies are typically sent along with the signature unless they are already extant at or available to the recipient. At the receiving end a verification takes place which includes utilization of the originator's public key, which has been obtained by the recipient with a certificate from a trustworthy source, and application of the hash function to the documents which are received or otherwise available.

An encryption of data employing the El-Gamal algorithm for the purpose of transmission to a recipient generally involves using the public key of the recipient, which has been obtained with a certificate from a trustworthy source, and a secret fresh random number. The data so encrypted may comprise a symmetric key for one time use which has been used to encrypt in a computationally efficient manner an associated item employing a symmetric encryption algorithm, the encrypted symmetric key and the associated item constituting a package. At the receiving end, the encrypted data or package is decrypted by operations including a decryption using the private key of the recipient. In the case of a package, the decryption using the private key yields the symmetric key which is then used to decrypt the associated item in a computationally efficient manner.

The need for secret fresh random numbers to be available at the user equipment, generally requires the expense of equipping all user equipment with a random number generator based on a natural random phenomenon, such as a reverse biased zener diode exhibiting shot noise in its current. This expense could be avoided if secret fresh random numbers were generated at the server and supplied to the user equipment via the network in a secure manner when needed. However, even if an encrypted channel were set up between the server and the user through an exchange of public keys, and a certificate system were in place to certify the public keys, thereby preventing a man-in-the-middle attack, the freshness requirement would still make the system vulnerable to a block replay attack, in which previous encrypted transmissions, or portions thereof, are replayed by an attacker.

In the aforementioned related patent application, it has been proposed that the private keys of users be maintained at the server in encrypted form, encrypted using user identifying keys, and supplied to the user or client equipment via the network only when needed, for example, for performing a digital signature or encryption. The user identifying keys are derived from user identifying information which is assumed to require the actual presence of the user at the user equipment, in particular a hash of a passphrase entered by the user or biometric information (fingerprint, voiceprint, retina scan, or face scan) measured or scanned by interaction with a physically present user.

In the prior art, also challenge response protocols are known for enabling a server to authenticate a client or user, i.e. to verify that the user possesses his private key, before showing the user any private information. Typically, a challenge response protocol consists of the server generating a random number and sending it in the clear via a network to the user, and the user responding by signing the random number using his private key and sending this signature back to the server. The server can verify the signature (and ensure that it was for the same random number that was sent) using the user's private key and the random number. However, if the El-Gamal algorithm were employed for the signature, there would have to be a random number generator at the user equipment to provide another random number to be used for the signature along with the user's private key. The random number to be signed could not also be used as the random number needed for an El-Gamal signature because of lack of assurance to the user equipment that this random number is both secret and fresh.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a method of administering and using secret fresh random numbers in which such random numbers are generated at the server and supplied to the user equipment in a secure manner when needed, for example, for digital signatures or encryptions employing the El-Gamal algorithm.

It is a further object of the present invention that one or more secret fresh random numbers are passed from the server to the user equipment in a manner which not only assures that the random numbers passed are secret and fresh, but also serves to authenticate the user to the server in the nature of a challenge response protocol.

It is another object of the present invention to provide such a random number administration and utilization method in conjunction with a method for administering and using private keys in which private keys of users are not retained on user equipment, but rather are retained in memory means accessible to the server and are transmitted to the user equipment in encrypted form via the network when needed, for example, for such digital signatures or encryptions employing the El-Gamal algorithm.

It is still another object of the present invention to provide a method of and system for administering secret fresh random numbers and private keys of users in a centralized manner and for distributing such random numbers and keys to user equipment in a manner which is highly secure from extraction and from block replay attack.

Briefly, these and other objects are satisfied by methods and systems in which there is associated with each user a respective set of a private key, public key corresponding to the private key, ID, and preferably a unique user identifying key which is obtainable only through interaction with a user that is physically present at the user equipment.

From the point of view of the server, the present invention is directed to a method of administration of secret fresh random numbers for use by users in a networked environment to which a server is coupled, said method both assuring that the random numbers are secret and fresh and also being in the nature of a challenge response protocol in which: a user's ID is received via the network; at least a first random number is generated and encrypted using the public key of the user; a freshness value corresponding to a current date/time is formed; items are hashed including the first random number and the freshness value to form a first hash; a first signature of the first hash is formed using the private key of the server; a package including an encrypted component containing at least the first random number, freshness value, and first signature is sent to the user via the network; and subsequently there is received a second signature of data derived from at least the first random number, said second signature being formed using the private key of the user; and using the public key of the user, it is first verified whether the second signature is for the same first random number as was sent by the server.

Further, in view of the use of the El-Gamal algorithm for all mentioned encryptions with a public key, and for all mentioned signatures with a private key, actually at least first, second, third, and fourth random numbers are generated and utilized in constructing the package. Specifically, in forming the package at the server, at least the first and second random numbers are contained in the encrypted component which is formed using the public key of the user and the third random number; the first hash is formed by hashing together the first and at least another of the random numbers contained in the package (including possibly the second random number) and the freshness value; the first signature of the first hash is formed using the private key of the server and the fourth random number. In regard to the subsequently received second signature of data, the data comprises a second hash which has been formed at the user equipment by hashing together the first and at least another of the random numbers contained in the package (including possibly the second random number), and the signature thereof has been formed using the private key of the user and the second random number. Then, the first verifying step is whether the second signature is for same random numbers as were sent by the server. This leaves the user equipment with at least the first random number which is fresh, secret, and consequently usable for a subsequent signature

or encryption operation, while also enabling the server to authenticate the user by the fact that the user was able to sign the first and at least another random number included in the package using his private key and the second random number.

As in the aforementioned related application, the method from the point of view of the server also involves reading from a storage means data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user. This encrypted private key of the user read from the storage means is included in the aforementioned package sent to the user. The user identifying information comprises a passphrase entered by the user at the user equipment, or biometric information which is obtained from the user by suitable measurement or scanning at the user equipment.

From the point of view of the user equipment, the present invention is directed to a method for obtaining and using secret fresh random numbers at user equipment in a networked environment to which a server is coupled, in which: an ID of a user is transmitted; a package is received including an encrypted component containing at least a first random number, which has been formed using the public key of the user, a freshness value corresponding to a date/time, and a first signature of a first hash, said first hash having been formed by hashing together items including said first random number and the freshness value, and said first signature having been formed using the private key of the server; at least the first random number is decrypted the using the private key of the user; it is determined whether the current date/time is no more than a predetermined amount later than the freshness value; the first hash is independently computed; the first signature is verified using the public key of the server and the independently computed first hash; and if the results of the determining and verifying are positive, a second signature of data derived from at least the first random number is formed using the private key of the user, and is sent to the server via the network.

As previously mentioned the received package actually has been constructed using at least first, second, third, and fourth random numbers, of which the encrypted component which has been formed using the public key of the user and the third random number contains at least the first and second random numbers, the first hash has been formed by hashing together said first random number, at least another of the random numbers included in the package (including possibly the second random number), and said freshness value, and the first signature thereof has been formed using the private key of the server and the fourth random number. Consequently, at the user equipment, the at least first and second random numbers are decrypted using the private key of the user, the data is formed by hashing together

the decrypted at least first and random number and another of the random numbers contained in the package (including possibly the second random number) to form a second hash, and the second signature thereof is formed using the private key of the user and the second random number.

Further, the method from the point of view of the server involves that the received package further includes the private key of the user encrypted with a user identifying key associated with the user, and that the encrypted private key is decrypted using a user identifying key determined from interaction with the user at the user equipment. The user identifying key determined by interaction with the user at the user equipment is determined from a passphrase entered by the user at the user equipment or biometric information which is obtained from the user by suitable measurement or scanning at the user equipment.

The present invention is also directed to a server system for supplying items for a plurality of users for use in signature or encryption operations employing the El-Gamal algorithm, which system comprises a random number generator for generating at least first, second, third, and fourth random numbers, and means for forming a package including: at least the first and second random numbers encrypted together using the public key of a user and the third random number; a freshness value; and a first signature of a first hash formed by hashing together said first and second random numbers and said freshness value, said first signature being formed using the private key of the server and the fourth random number. The server system is also characterized in that it further comprises verification means for verifying received second and third signatures, the second signature being of a second hash which has been formed by hashing together the first and at least another random number contained in the package, and having been made using the private key of the user and the second random number, and the third signature being of a hash of a document, and having been made using the private key of the user and the first random number. Also, the server system comprises computer readable storage means characterized in that there is stored therein encrypted private keys for the respective users which private keys have been encrypted using respective keys determined from respective user identifying information (e.g. a passphrase or biometric information), and wherein the package further includes the encrypted private key of the user.

Other objects, features and advantages of the present invention will become apparent upon perusal of the following detailed description when taken in conjunction with the appended drawing, wherein:

BRIEF DESCRIPTION OF THE DRAWING

Figure 1 is a schematic diagram of an exemplary system in accordance with the present invention for administering random numbers and private keys for a plurality of users used for digitally signing documents employing the El-Gamal algorithm, which system includes user equipment and a server; and

Figure 2 is a data flow chart which indicates in separate columns the method steps performed by the user, the user equipment, and the server in operation of the system of Figure 2.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

It should be understood that while the present invention is discussed hereinafter in terms of an exemplary system and method for obtaining digitally signed documents of a plurality of users in a networked environment which have been signed employing the El-Gamal algorithm, the principles of the present invention are equally applicable to distribution of secret fresh random numbers, and/or to distribution of a combination of a secret fresh random number and an encrypted private key, for other purpose. Further, when used for digital signatures, it should be appreciated that such signatures may be applied to a variety of data, files, programs or other "documents", whether originated, modified or reviewed by users. In any event, the digital signature may be thought of as manifesting an approval by the user of a document.

One aspect of the present invention is that it employs user identifying keys Kpass for each user, for securing private keys KprUser. The user identifying keys Kpass can only be derived from user identifying information obtained by interaction with the user physically present at the user equipment. The user identifying information may be either a fanciful series of words, termed a passphrase, entered by a user or biometric information, such as a fingerprint, voiceprint, retina scan or face scan, obtained by measurement or scanning of the user.

It is very difficult to guess passphrases as opposed to passwords as there are many possible phrases. For example, a particularly good passphrase may concatenate two phrases which are in different languages. Guessing such a passphrase would be extremely difficult using normally available computer power. Also, biometric information is particularly unique and immune to a guessing attack.

Referring first to Figure 1 of the drawing, there is shown a networked system 10 comprised of a plurality of computer stations, terminals or other user computing and/or communication equipment 12 and a server 16 interconnected or capable of communicating via a wired or wireless network 14. A store 18, which may be or include RAM, ROM, a hard disk, or other memory or media, is coupled to or forms part of server 16, and contains respective sections 18a-e, or fields in a data structure, for storing user IDs, encrypted private keys, public keys, documents, and digital signatures, respectively, for all users, which are indexed or otherwise addressable or retrievable by ID. Networked system 10 may take a variety of forms but is preferably an intranet, the network 14 supporting TCP/IP, the user equipment 12 employing web browsers, and the server 16 acting as a web server.

The public/private key pair for each user is implemented pursuant to the well known El-Gamal algorithm or public key cryptosystem, whereas the encrypted private keys stored in section or field 18b of the store 18 have been encrypted with a symmetric encryption/decryption algorithm (employing the same key for encryption and decryption) such as IDEA or DES using a user identifying key derived from the user's passphrase or biometric information.

In accordance with the El-Gamal algorithm, the public key actually consists of three components, Y, G and P, and the private key consists of a random number X, where P is a prime number, G is a random number, and $Y=G^X \bmod P$. For the purposes of the present invention, preferably prime number P has a length of 1024 bits, and all random numbers generated for use in signature or decryption using the El-Gamal algorithm (R1, R2, R3, R4 referred to hereinafter) have a length of 128 bits. It is a further requirement of the El-Gamal algorithm that these generated random numbers be invertible in the finite field of numbers described by the length of P, i.e 1024 bits.

In order to construct the dataset of encrypted private keys E[Kpass](KprUser), the user identifying keys Kpass have previously been obtained in an extremely secure way as a result of the presence of the respective users at secure equipment 20 coupled to store 18 or server 16. Secure equipment 20 comprises a user interaction means 20a and a hashing means 20b of the same form as the user interaction means 12a and hashing means 12b, respectively, of user equipment 12 (which will be described hereinafter), a key generator 20c for generating public key/private key pairs KpuUser/KprUser, and an encryption means for encrypting a generated private key KprUser with a user identifying key Kpass using a symmetric encryption algorithm such as IDEA or DES.

At the secure equipment 20, using the user interaction means 20a each passphrase was entered by the respective user or biometric information obtained by measuring or scanning the respective user in front of the system administrator (to confirm the user's identity) when the user was assigned a private key KprUser and a corresponding public key KpuUser generated by key generator 20c, but any passphrase entered or biometric information obtained was not viewed by or accessible to the administrator. The entered passphrase or obtained biometric information was then immediately hashed by hashing means 20b with a secure hash function (SHA-1 or RIPEMD) to form a fixed length user identifying key Kpass, of at least 128 bits in length (160 bits if SHA-1 is used), which was immediately used by encryption means 20c to encrypt the assigned private key KprUser with the symmetric algorithm, after which all traces of the entered passphrase or obtained biometric information, and the hash thereof were cleaned from the secure equipment 20. Further, IDs are assigned at the same time as the thereby encrypted private keys E[Kpass](KprUser), and the corresponding public keys KpuUser, these items being stored in sections or fields 18a, 18b, and 18c, respectively.

User equipment 12 includes: input interaction means 12a such as a mouse and/or keyboard, handwriting recognition, voice recognition or other input means for obtaining an ID and, if used, a passphrase from a user, and for a user to fill in a document, and for biometric measurement or scanning, if used, to obtain biometric information (fingerprint, voiceprint, retina scan, face scan) from a user; a hashing means for applying a secure hash function (SHA-1 or RIPEMD) to an entered passphrase or obtained biometric information, and to an approved document; a symmetric decryption means 12c for decrypting an encrypted private key received from server 16 using the hashed passphrase or biometric information as a user identifying key; and an El-Gamal algorithm means 12d for performing encryption, decryption, signature and verification operations in accordance with the El-Gamal algorithm, the encryption and signing operations requiring secret fresh random numbers. In particular, as will become clearer as the discussion proceeds, El-Gamal algorithm means performs decryption, verification, and signature operations in conjunction with a challenge response protocol assuring to the user equipment 12 that a random number R1 supplied to from server 16 is both secret and fresh, and assuring to the server that the user is in possession of the private key (i.e. was able to decrypt the private key because the correct user identifying information has been obtained by user equipment 12). Thereafter, a document is sent for approval, possibly after modification or filling in, a hash of the approved document is signed using the private key of the user and this secret fresh random number R1 to form a digital

signature S[KprUser, R1](H(DOC)) of a document. The various hashing, symmetrical decryption, and El-Gamal algorithm means 12b, 12c, 12d may be implemented by software running on a CPU (not shown) of user equipment 12 or by special purpose hardware. Where the system 10 is implemented as an intranet, this functionality would be carried out by an applet supplied by server 16. It should be understood that in order to prevent a man-in-the-middle attack, the applet must be signed by the server and verified at user equipment 12 using the public key of the server KpuServer obtained with a certificate from a trusted authority.

Server 16 comprises: means 16a for reading from and writing to the store 18; random number generator means 16b for generating random numbers; hashing means 16c for performing a secure hash function to hash together random numbers and other items in conjunction with the challenge response protocol, and for forming a hash of a received approved document H(DOC); El-Gamal algorithm means 16d for performing encryption, decryption, signature, and verification operations employing the El-Gamal algorithm, the encryption and signing operations requiring secret fresh random numbers; and a freshness value generating means 16e for constructing a freshness value FR indicating a date/time assigned to items or a package being transmitted by server 16. Random number generator 16b is preferably a natural random source which reads or measures a natural random phenomenon, e.g. shot noise in the current of a reverse biased zener diode. Hashing means 16c, El-Gamal algorithm means 16d, and freshness value generating means 16e may be implemented by software running on a CPU (not shown) of server 16, or by specialized hardware.

The operation of the networked system 10 in providing a secret fresh random number R1 and encrypted private key KprUser to the user in the course of a phase in the nature of a challenge response protocol, which after completion of this phase, are used for a digital signature employing the El-Gamal algorithm of a document S[KprUser, R1](H(DOC)) which is derived from, or the same as, a then supplied document, will be best understood by also referring to Figure 2. This Figure shows the operations performed by user interaction, by the user equipment 12, and by the server 16 in different columns. For the purposes of this Figure, it is assumed that the user has already requested access to the document system (home page) and the server 16 has sent a sign-in page to the user equipment 12. Thereafter at step 30, the user enters his ID in the sign-in page via input means 12a, e.g. the initials of the user, providing the IDs of all users are unique, and at step 40 the sign-in page including the entered ID is transmitted to the server, which receives it at step 70. In response, at step 72 the server 16, using the received ID as an index, reads from store 18 the corresponding encrypted private key E[Kpass](KprUser) and public key KpuUser of the user. Also at step 74, random number

generator 16b generates four random numbers R1, R2, R3, and R4 and freshness value generating means 16e forms a freshness value FR representing the current date/time by checking the clock (not shown) of server 16.

The items obtained in steps 72, and 74 are used in step 76 using hashing means 16c and El-Gamal algorithm means 16d to form a package of items which is then transmitted to user equipment 12 via network 14. The package consists of:

a) a first encrypted component E1 read in step 72 which as aforementioned has previously been formed by encrypting the private key of the user KprUser using the user's identifying key Kpass:

E1 = E[Kpass](KprUser);

b) a second encrypted component E2 which is formed by the server encrypting together random numbers R1 and R2 employing the El-Gamal algorithm using the public key of the user KpuUser and the third random number, thereby forming:

E2 = E[KpuUser, R3](R1, R2);

c) freshness value FR; and

d) a first signature S1 of a hashing together of the first and second random numbers R1, R2, and the freshness value FR, which signature employs the El-Gamal algorithm using the private key of the server KprServer and the fourth random number R4, thereby forming:

S1 = S[KprServer, R4](H(R1, R2, FR).

There are a variety of techniques known to persons of ordinary skill in the art to encrypt together multiple items or to hash together multiple items. A sufficient method in each case is to concatenate the multiple items prior to the encrypting or hashing operations.

The package may also contain the public key of the server KpuServer and certificate pertaining thereto from a trustworthy authority needed by user equipment 12.

At user equipment 12, the package is received at step 44, and prior to after step 44, the user identifying information is obtained at step 32 by user interaction means obtaining an entered passphrase or scanning or measuring biometric information (fingerprint, voiceprint, retina scan, or face scan) with respect to the user physically present at user equipment 12, and at step 42, employing hashing means 12b to apply the same secure hash function (SHA-1 or RIPEMD) to the user identifying information as was applied by hashing means 20b of secure equipment 20, to thereby obtain the same user identifying key Kpass as was utilized in producing the received encrypted private key E[Kpass](KprUser).

In step 46, symmetric decryption means 12c is employed using the obtained user identifying key Kpass to decrypt the received first encrypted component E1 to obtain the private key KprUser of the user, which operation is represented as follows:

D[Kpass](E[Kpass](KprUser)) = KprUser, and

the El-Gamal algorithm means 12d is employed using the thereby obtained private key KprUser to decrypt the received second encrypted component E2 to obtain the first and second random numbers R1 and R2. The latter operation is represented as follows:

D[KprUser](E[KpuUser, R3](R1, R2)) = R1, R2.

Further, at step 50, the current date/time of the user equipment clock (not shown) is read and compared with the received freshness value FR. If the current date/time is not later than the freshness value by more than a predetermined amount, determined from a maximum permitted delay between freshness value generation in step 74 and freshness value checking in step 50, the received package is considered fresh. For the purposes of the freshness test it must be assured that the clocks on the server 16 and user equipment 12 are closely aligned, and the time to perform an entire challenge response protocol exceeds the maximum permitted delay. Also, at step 52 hashing means 12b are utilized to hash together random numbers R1 and R2, and the freshness value FR, and this hash together with the public key of the server KpuServer are used in a verification operation by El-Gamal algorithm means 12d of the received first signature S1. The verification operation may be represented as:

V[KpuServer, H(R1, R2, FR), S1] = pass or fail.

If the aforementioned verification and freshness tests are passed, in step 54 a second signature S2 is formed utilizing hashing means 12b and El-Gamal algorithm means 12d, which second signature S2 is transmitted to server 16 via network 14. In this step, the El-Gamal algorithm is employed using the private key of the user KprUser and the second random number R2 to sign a hashing together of the first and second random numbers R1, R2. The resultant second signature S2 is represented as follows:

S[KprUser, R2](H(R1, R2)).

At the server, this second signature S2 is verified at step 78 by first using hashing means 16c to independently compute a hashing together of random numbers R1, R2 and then using this hash and the read public key of the user KpuUser in a verification operation of El-Gamal algorithm means 16d. This second verification operation, which completes the challenge response protocol by enabling the server to authenticate the user, is represented as follows:

V[KpuUser, H(R1, R2), S2] = pass or fail

In the combined random number passing and challenge response protocol of the present invention, the random numbers R1, R2 have been encrypted by the server to prevent an attacker from getting the numbers and discovering the user's private key KprUser from a signature or encryption by the user using the private key. The freshness value has been sent to assure the freshness of the encrypted random numbers. These random numbers R1, R2 and the freshness value FR have been signed by the server (in forming the first signature S1) to prove that:

a) the random numbers are from the server, otherwise an attacker could send random numbers to the user equipment, and because he already knows them, could discover the user's private key from a signature or encryption by the user using the private key; and

b) the freshness value corresponds to these random numbers, otherwise an attacker could get an old signed set of random numbers and attach a new freshness value to them.

If the verification test in step 78 is passed, in step 80 a document to be filled out (or merely approved without modification) by the user is read from store 18d and sent to user equipment 12 via network 14, where it is received at step 56. If the document is accompanied by or forms part of a further applet, as previously mentioned, the applet should be signed by the server 16 and verified at user equipment 12 employing the public key of the server KpuServer.

The completion, signature and verification of the document proceeds in an essentially conventional manner. Through user input at step 34 via user interaction means 12a, the document is filled in, or merely reviewed, and the user's approval of the completed or merely reviewed document DOC is indicated. To manifest this completion and/or approval, in step 80 a third digital signature S3 is formed by using hashing means 12b to produce a hash of the approved document DOC and applying the signature operation of El-Gamal algorithm means 12d thereto using the private key of the user KprUser and the first random number, to form a third signature which is represented as follows:

S[KprUser, R1](H(DOC)).

The third signature S3 and the approved document DOC are at step 62 sent to the server 16, where hashing means 16c are employed to independently compute a hash of the received approved document DOC, and the El-Gamal algorithm means is employed to perform a verification operation using this hash H(DOC) and the public key of the user KpuUser. The verification operation is represented as follows:

V[KpuUser, H(DOC), S3] = pass or fail.

If the verification operation is passed, in step 84, the approved document DOC and the signature S3 are saved in sections 18d, 18e, respectively, of store 18.

Lastly, at user equipment 12, in step 64 in order to frustrate an attacker attempting to compromise the system, any record of the decrypted random numbers R1, R2, the decrypted private key KprUser, the entered passphrase or obtained biometric information, or the user identifying key Kpass formed therefrom, are all erased or destroyed (or, alternatively, a non-volatile record is never made) so they cannot be obtained from the user equipment.

An interesting extension of the system described thus far is possible where the user will need multiple random numbers to sign multiple documents. This extension comes from the recognition that because the data encrypted in the package can have a length of just less than the length of the prime number P, allowing some room for padding, actually at little computational cost further random numbers in addition to R1 and R2 may be encrypted together and signed together with freshness FR in the package formed in step 76. For example, given P having a length of 1024 bits, and the random numbers having a length of 128 bits, five further random numbers R5, R6, R7, R8, and R9 could be so sent at the same time. This would involve that nine random numbers be generated at step 74 and that the second encrypted component E2 in the package formed in step 76, would instead be:

E2 = E[KpuUser, R3](R1, R2, R5, R6, R7, R8, R9).

These seven encrypted random numbers R1-R2, and R5-R9 would be decrypted by the user equipment at step 46, and with the use of random number R2 to form the second signature S2, six random numbers R1 and R5-R9 would be available for signatures of documents.

Further, the signature S1 in the package formed and sent by the server at step 76 could be a hashing together of the freshness and the aforementioned seven random numbers, but it would be sufficient to sign a hashing together of the freshness FR and at least two of these random numbers. Similarly, a sufficient signature S2 formed and sent by the user equipment 12 in step 54 would be of a hash of at least two of the random numbers received.

Where more than six random numbers are needed for digital signatures, it is also possible to generate further additional random numbers in step 74 and include them in one or more further encrypted components in the package formed and sent by the server in step 76.

It should now be appreciated that the objects of the present invention have been satisfied and that the present invention provides a secure protocol for distributing random numbers and private keys for digital signatures in a networked environment such as an intranet

system which can only be compromised by a passphrase or biometric information guessing attack, which is fairly hard, or by failure of the El-Gamal algorithm.

While the present invention has been described in particular detail, it should also be appreciated that numerous modifications are possible within the intended spirit and scope of the invention. For example, the present invention is equally applicable to systems where IDs do not have to be entered by users because they may be retained at user equipment.

CLAIMS:

1. A method of administration of secret fresh random numbers for use by users in a networked environment (14) to which a server (16) is coupled, there being associated with each user a unique respective set including an ID, a private key (KprUser), and a public key (KpuUser) corresponding to the private key (KprUser), and with the server (16) a private key (KprServer) and a public key (KpuSever), said method comprising, at the server (16):

receiving (70) via the network (14) a user's ID;

generating (74) at least a first random number (R1);

forming (76) an encrypted component (E2) using the public key (KprUser) of the user, said encrypted component (E2) containing at least the first random number (R1) in encrypted form;

forming (74) a freshness value (FR) corresponding to a current date/time; hashing together (78) items including the first random number (R1) and the freshness value (FR) to form a first hash;

forming (76) a first signature (S1) of the first hash using the private key of the server (KprServer);

sending to the user via the network (14) a package including at least the encrypted component (E1), freshness value (FR), and first signature (S1);

receiving a second signature (S2) of a second hash which has been formed (54) by signing data derived at least from the first random number (R1), said second signature (S2) being formed using the private key of the user (KprUser); and

first verifying (78), using the public key (KpuUser) of the user, whether the second signature (s2) is for the same first random number (R1) as was sent by the server (16).

2. The method as claimed in Claim 1, wherein:

in addition to said first random number (R1), at least second (R2), third (R3), and fourth (R4) random numbers are generated;

at least the first and second random numbers (R1, R2) are encrypted using the public key (KpuUser) of the user and the third random number (R3);

said first hash is formed by hashing together at least said first random number (R1), another random number (R2) contained in the package in encrypted form, and said freshness value (FR);

said first signature (S1) of the first hash is formed (76) using the private key of the server (KprServer) and the fourth random number (R4);

said data is formed by hashing together the first (R1) and at least another (R2) random number contained in said package in encrypted form to produce a second hash;

said second signature (S2) of the second hash has been formed using the private key (KprUser) of the user and the second random number (R2).

3. The method as claimed in Claims 1 or 2, further comprising reading (72) from a storage means (18) data corresponding to the user having the received ID, which data comprises the user's private key (KprUser) encrypted using a key (Kpass) determined from identifying information of the user, and said package further includes the encrypted private key of the user.

4. The method as claimed in Claim 3, wherein the user identifying information comprises a passphrase entered by the user at the user equipment (12), or biometric information which is obtained from the user by suitable measurement or scanning at the user equipment (12).

---

5. The method as claimed in Claim 4, further comprising receiving a third signature (S3) of a third hash of a document (DOC), which third signature (S3) has been formed (60) using the private key of the user (KprUser) and the first random number (R1), and second verifying (82) the third signature (S3) using the public key (KpuUser) of the user and an independently computed hash of the document (DOC).

6. A method for obtaining and using secret fresh random numbers at user equipment (12) in a networked environment (14) to which a server (16) is coupled, there being associated with each user a unique respective set including an ID, a private key (KprUser), and a public key (KpuUser) corresponding to the private key (KprUser), and with the server a private key (KprServer) and a public key (KpuUser), said method comprising, at the user equipment (12):

transmitting (40) an ID of a user;

receiving (44) a package including an encrypted component (E2) containing at least a first random number (R1) in encrypted form, which encrypted component (E2) has been produced using the private key (KprUser) of the user, a freshness value (FR) corresponding to a date/time, and a first signature (S1) of a first hash, said first hash having been formed (76) by hashing together items including said first random number (R1) and the freshness value (FR), and said first signature (S1) having been formed (76) using the private key (KprServer) of the server;

decrypting (46) the at least first random number (R1) using the public key (KpuUser) of the user;

determining (50) whether the current date/time is no more than a predetermined amount later than the freshness value (FR);

independently computing (52) the first hash;

verifying (52) the first signature using the public key of the server (KpuServer) and the independently computed first hash; and

if the results of the determining and verifying (52) are positive:

forming (54) a second signature (S2) of data derived from at least the first random number (R1) using the private key of the user (KprUser); and

sending the second signature (S2) via the network.

7. The method as claimed in Claim 6, wherein:

said encrypted component (E2) contains at least first and second random numbers (R1, R2) which have been encrypted together using the public key (KprUser) of the user and a third random number (R3);

said first hash has been formed by hashing together at least said first random number (R1), another random number (R2) contained in said package, and said freshness value (FR);

said first signature (S1) of the first hash has been formed using the private key (KprServer) of the server and a fourth random number (R4);

at least said first and second random numbers (R1, R2) are decrypted (46) from the encrypted component (E2) using the private key (KprUser) of the user;

said data is formed (54) by hashing together at least two of the random numbers (R1, R2) contained in said package in encrypted form to produce a second hash;

said second signature (S2) of the second hash is formed using the private key (KprUser) of the user and the second random number (R2).

8. The method as claimed in Claim 6, wherein said package further includes the private key of the user encrypted with a user identifying key (Kpass) associated with the user, and said method further comprises decrypting (46) the encrypted private key using a user identifying key (Kpass) determined from interaction with the user at the user equipment (12).

9. The method as claimed in Claim 8, wherein the user identifying key (Kpass) determined by interaction with the user at the user equipment (12) is determined from a passphrase entered by the user at the user equipment (12) or biometric information which is obtained from the user by suitable measurement or scanning at the user equipment (12).

10. The method as claimed in Claims 8, further comprising:

computing (54) a third hash of a document (DOC);

forming (54) a third signature (S3) of the third hash using the user's private key (KprUser) and the first random number (R1); and

transmitting (54) the third signature (S3).

11. A server system for supplying items for a plurality of users for use in signature or encryption operations employing the El-Gamal algorithm, there being associated with each user a unique respective set including a private key (KprUser), and a public key (KpuUser) corresponding to the private key (KprUser), and with the server a private key (KprServer) and a public key (KprServer), said system comprising:

a random number generator (16b) for generating at least first, second, third, and fourth random numbers (R1, R2, R3, R4); and

means (16c, 16d, 16e) for forming (76) a package including an encrypted component (E2) containing at least the first and second random numbers (R1, R2) encrypted together using the public key (KpuUser) of a user and the third random number (R3); a freshness value (FR); and a first signature (S1) of a first hash formed by hashing together said first random number (R1), at least another random number (R2) contained in said package in encrypted form, and said freshness value (FR), said first signature (S1) being formed using the private key (KprServer) of the server and the fourth random number (R4).

12. The system as claimed in Claim 11, further comprising verification means (16d) for verifying (78, 82) received second and third signatures (S2, S3), said second signature (S2)

being of a second hash which has been formed by hashing together the first (R1) and at least another random number (R2) contained in said package, and having been made (54) using the private key (KprUser) of the user and the second random number (R2), and said third signature (S3) being of a hash of a document (DOC), and having been made (60) using the private key of the user (KprUser) and the first random number (R1).

13. The system as claimed in Claim 12, further comprising computer readable storage means (18) characterized in that there is stored therein (18b) encrypted private keys for the respective users which private keys (KprUser) have been encrypted using respective keys (Kpass) determined from respective user identifying information, and wherein said package further includes the encrypted private key of the user (E1).

14. The system of Claim 13, wherein the user identifying information comprises a passphrase or biometric information.

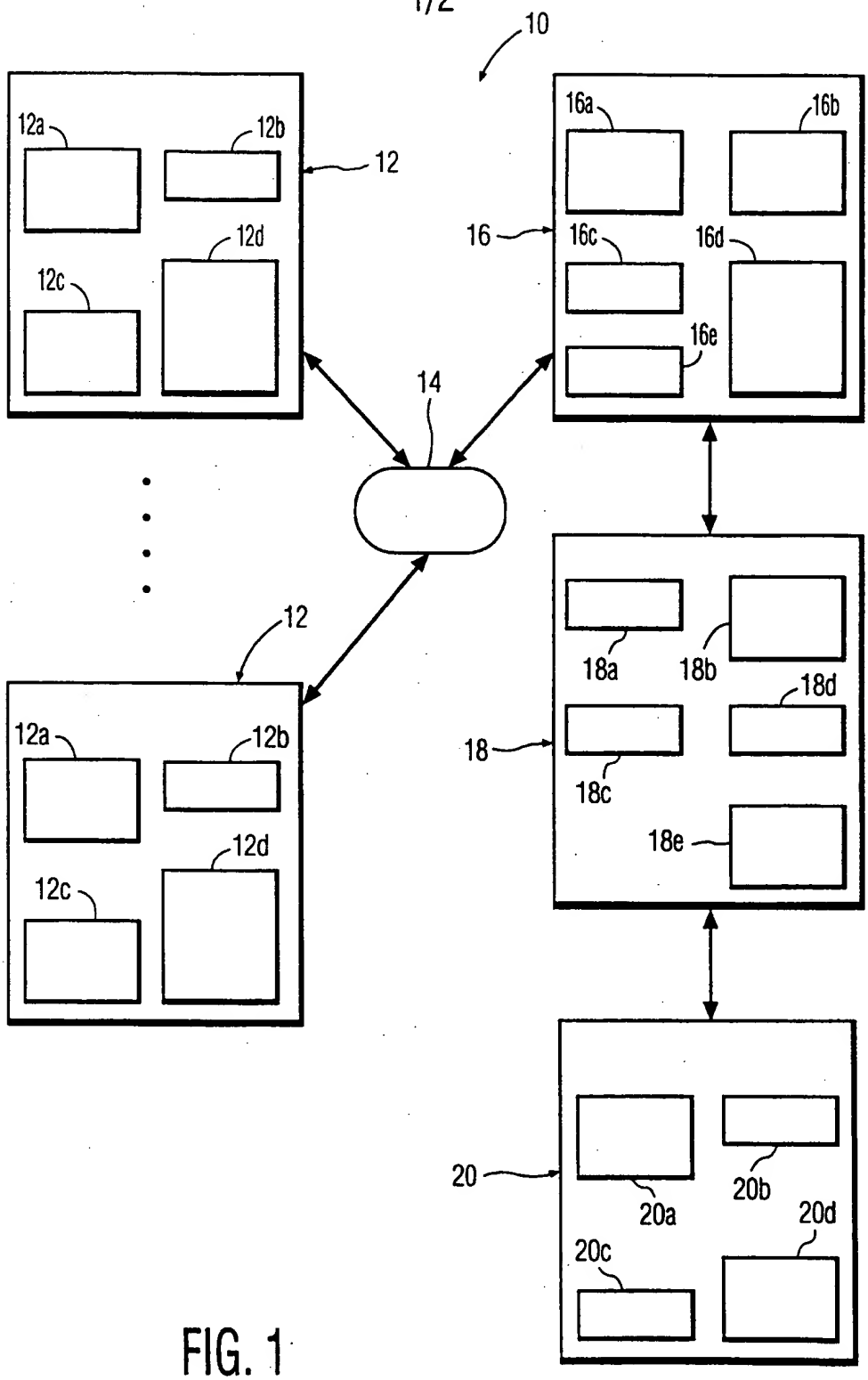
10
12a
12b
12
12d
12c
16a
16b
16
16c
16d
16e
14
12
12a
12b
12d
12c
18a
18b
18d
18
18c
18e
20
20a
20b
20d
20c

FIG. 1

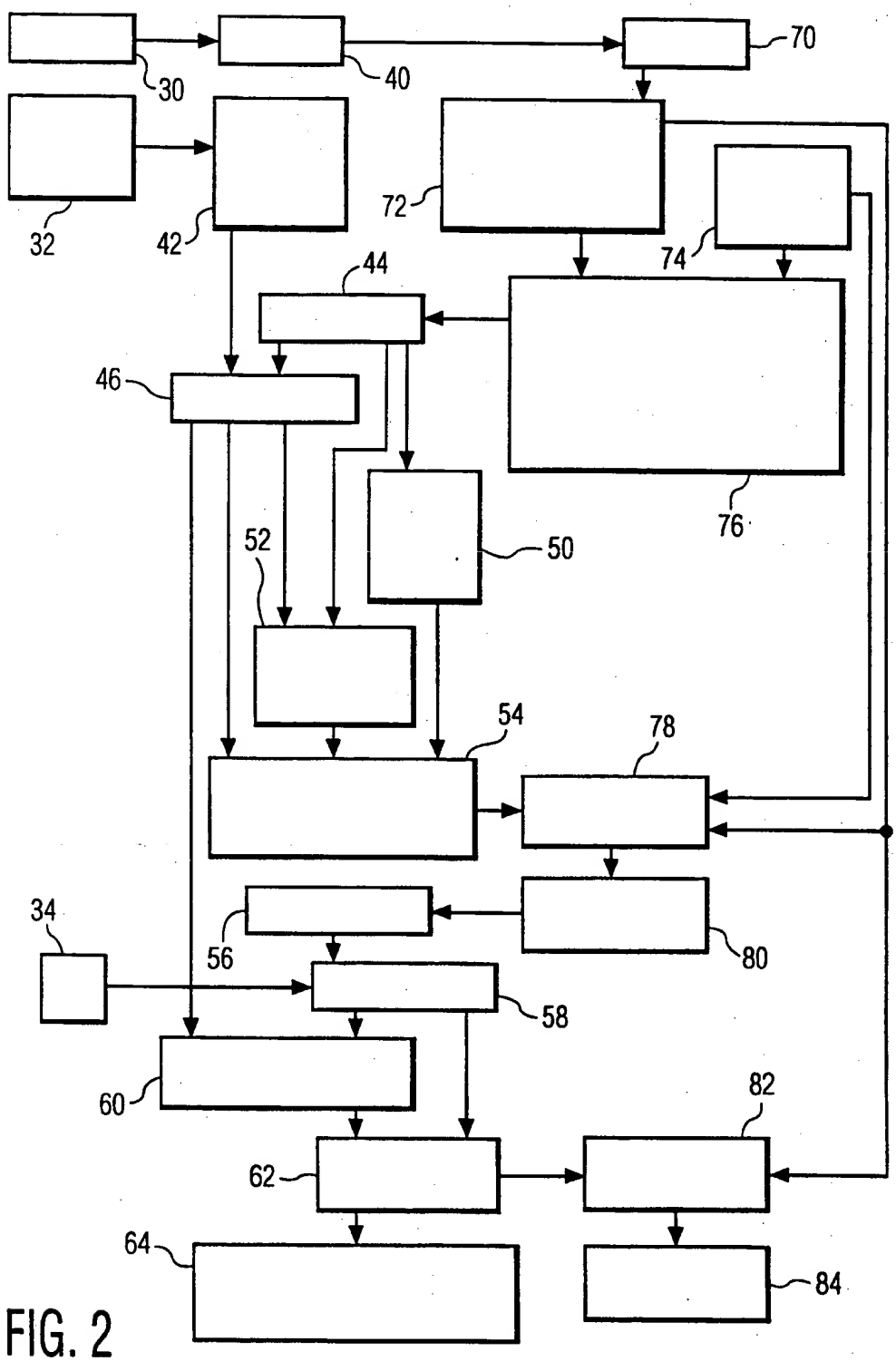

FIG. 2

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/30, 9/32	A3	(11) International Publication Number: WO 99/34554
		(43) International Publication Date: 8 July 1999 (08.07.99)

(21) International Application Number: PCT/IB98/01923

(22) International Filing Date: 3 December 1998 (03.12.98)

(30) Priority Data:
08/989,875 24 December 1997 (24.12.97) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Applicant *(for SE only)*: PHILIPS AB [SE/SE]; Kottbygatan 7, Kista, S-164 85 Stockholm (SE).

(72) Inventors: CUCCIA, David; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). EPSTEIN, Michael, A.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). PASIEKA, Michael, S.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: FAESSEN, Louis, M., H.; Internationaal Octrooibureau B.V., P.O. Box 220, NL-5600 AE Eindhoven (NL).

(81) Designated States: CN, JP, KR, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(88) Date of publication of the international search report:
10 September 1999 (10.09.99)

(54) Title: ADMINISTRATION AND UTILIZATION OF SECRET FRESH RANDOM NUMBERS IN A NETWORKED ENVIRONMENT

(57) Abstract

In a public key cryptosystem employing the El-Gamal algorithm, secret fresh random numbers are generated at a server and private keys of users, as encrypted with a symmetric algorithm by using individual user identifying keys determined by hashing the users' respective passphrases or biometric information (fingerprint, voiceprint, retina scan, or face scan) are maintained in a store accessible to the server, and the fresh random numbers and encrypted private keys are transmitted to the user equipment when needed via a network which is not secure. In order to prevent an attacker from discovering the random numbers or employing formerly used random numbers in a block replay attack, an interchange in the nature of a challenge response protocol is employed which passes at least one secret fresh random number from the server to the user equipment while also authenticating the user to the server. In this interchange, a first random number to be distributed to the user for use in signing a document and a second random number which is to be used by the user in forming a signature of a hashing together of the first and second random numbers as part of the challenge response protocol, are supplied to the user equipment in encrypted form together with a freshness value, and a signature by the server of a hashing together of the first and second random numbers and the freshness value.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 98/01923

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/30, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5434918 A (KENNETH C. KUNG ET AL), 18 July 1995 (18.07.95), abstract	1,3,4
A	--	2,5-14
A	Patent Abstracts of Japan, abstract of JP 7-325785 A (FUJITSU LTD), 12 December 1995 (12.12.95)	1-14
	--	
A	US 5481612 A (MIREILLE CAMPANA ET AL), 2 January 1990 (02.01.90), column 4, line 18 - line 61, abstract	1-14
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 June 1999	02 -07- 1999
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Bengt Romedahl/MN Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 98/01923

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5384848 A (HIROAKI KIKUCHI), 24 January 1995 (24.01.95), column 4, line 6 - line 46, abstract -- --------	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/06/99

International application No.
PCT/IB 98/01923

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5434918 A	18/07/95	AU 676107 B	27/02/97
		AU 1261595 A	03/07/95
		CA 2153879 A,C	22/06/95
		EP 0683907 A	29/11/95
		JP 8502847 T	26/03/96
		NO 953143 A	10/08/95
		WO 9516947 A	22/06/95
US 5481612 A	02/01/90	EP 0606792 A	20/07/94
		FR 2699300 A,B	17/06/94
US 5384848 A	24/01/95	GB 2276471 A,B	28/09/94
		JP 6266670 A	22/09/94